Headquarters
United States Army Recruiting Command
Fort Knox, Kentucky 40121-2726
16 October 2002

*USAREC Regulation 380-4

Effective 1 November 2002

Security

Security Program

For the Commander:

WANDA E. WILSON
Colonel, GS
Chief of Staff

Official:

ROGER H. BALABAN
Director, Information Management

History. This UPDATE printing publishes a revised regulation which is effective 1 November 2002.

Summary. This regulation prescribes policies and guidance pertaining to security programs which include personnel, physical, information, security education and awareness, Subversion and Espionage Directed Against the U.S. Army, and reporting incidents involving United States Army Recruiting Command personnel and facilities. This regulation also assigns responsibility for the protection of Army information, personnel, and property. This regulation does not include specific requirements for Army applicant personnel security procedures.

Applicability. This regulation applies to all military and civilians at all levels of the United States Army Recruiting Command. Any violation of its requirements may subject soldiers to disciplinary action under Article 92, Uniform Code of Military Justice, and civilian personnel may be subject to adverse action under civilian personnel regulations. Questions pertaining to this regulation or DOD and DA security regulations should be addressed to the Command Security Manager, DSN 536-0238 or 0225 or commercial (502) 626-0238 or 0225. Written inquiries should be forwarded to Commander, United States Army Recruiting Support Brigade (RCRS-SEC), Fort Knox, KY 40121-2726.

Proponent and exception authority. The proponent of this regulation is the Commander of the United States Army Recruiting Support Brigade. The proponent has the authority to approve exceptions to this regulation that are consistent with controlling law and regulation. Proponent may delegate the approval authority, in writing, to the executive officer within the proponent agency in the grade of lieutenant colonel.

Army management control process. This regulation contains management control provisions in accordance with AR 11-2 but does not identify key management controls that must be evaluated.

Supplementation. Supplementation of this regulation is prohibited.

Suggested improvements. The proponent agency of this regulation is the Office of the Commander of the United States Army Recruiting Support Brigade. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Cdr, RS Bde (RCRS-SEC), Fort Knox, KY 40121-2726.

Distribution. Distribution of this regulation has been made in accordance with USAREC Pam 25-30, distribution A. This regulation is published in the Recruiting Station Administration UPDATE.

Contents (Listed by paragraph number)

Chapter 1
General

1-1. Purpose

This regulation prescribes policies, guidance, and implements the United States Army Recruiting Command's (USAREC's) security programs including security inprocessing and outprocessing, personnel security (PS), information security, Subversion and Espionage Directed Against the U.S. Army (SAEDA), physical security (PHS), information system secu-

*This regulation supersedes USAREC Regulation 380-4, 6 April 2000.

rity, and incident reporting. This regulation combines security-related programs into one directive. This information is designed to supplement detailed instructions contained in references and establish policy specifically for USAREC.

1-2. References
Required and related publications and prescribed and referenced forms are listed in appendix A.

1-3. Explanation of abbreviations
Abbreviations used in this regulation are explained in the glossary.

1-4. Responsibilities

a. The USAREC Security Program is a command responsibility. It is also the responsibility of all military and civilian supervisors as well as individuals within USAREC. Commanders and supervisors must become familiar with the provisions of this regulation and implement applicable portions.

b. In order to implement a comprehensive security program, appointed security representatives and security managers (SMs) at all levels must have on hand and maintain the appropriate references cited in this regulation.

c. Commanders and directors will appoint SMs and security representatives (e.g., SMs, PHS officers, incident reporting officers, key custodians, etc.,), in writing, as appropriate. A copy of each appointment or changes to appointments will be forwarded to Headquarters, United States Army Recruiting Support Brigade (HQ RS Bde) (RCRS-SEC), Fort Knox, KY 40121-2726, as they occur. Appointed duties may be performed by either military or civilian personnel.

d. Commanders and directors will develop and implement comprehensive written standing operating procedures (SOPs) for applicable security programs for their activities.

e. The United States Army Recruiting Support Brigade (RS Bde) security officer serves as the SM for assigned Headquarters, United States Army Recruiting Command (HQ USAREC) security programs; manages the HQ RS Bde Security Division; and serves as the principal staff officer and point of contact for security-related matters for USAREC activities. The security officer provides guidance, policy, and assistance to field commanders and appointed SMs as required. As such, he or she may conduct security-related investigations, inquiries, commandwide inspections, staff visits, training, seminars, and establish policies required by regulation, directives, or as directed by the commander. The security officer reviews security posture at recruiting brigades (Rctg Bdes) and recruiting battalions (Rctg Bns).

f. Rctg Bde, Rctg Bn, and recruiting company (Rctg Co) commanders will establish and implement security programs within their respective activities in accordance with Army regulations, this regulation, and established SOPs. When required, commanders will coordinate security program requirements and issues or concerns with the HQ RS Bde Security Division. Rctg Bdes and Rctg Bns that have installation support agreements (ISAs) for intelligence and security services and/or police and law enforcement services must ensure that all aspects of requirements contained in Department of the Army (DA) and USAREC security regulations are met. Rctg Bdes and Rctg Bns must continually review their ISAs to determine what programs are supported and to what extent these programs are supported. Functional areas not specifically supported remain the responsibility of the Rctg Bde or Rctg Bn commander. Activities that have an ISA which include security program functions will provide a copy of the ISA to the HQ RS Bde Security Division. Copy of ISA changes, updates, and revisions must also be provided.

g. All personnel (civilian, military, and contractor) assigned or attached to USAREC have the inherent responsibility to be security conscious, to safeguard both classified and unclassified information and Government property. Included is the responsibility to report and/or correct actual or possible violations, reportable incidents, or inadequate security measures.

1-5. Coordination
Direct coordination between organizations, offices, or activities within USAREC is authorized and encouraged. In addition, Rctg Bdes and Rctg Bns may coordinate directly with local supporting security offices and law enforcement agencies on matters of security regulation and policy.

1-6. Reports
Specific reports and other written requirements are contained in each chapter of this regulation and cited Army regulations. All USAREC personnel are required to report within 24 hours, to the HQ RS Bde Security Division or their appointed unit SM, any actual, suspected, or possible compromise of classified information or sensitive information; security violation or incident, known or suspected attempts or contacts by unauthorized persons, agencies, or governments; and any other suspicious acts which may impact on security.

Chapter 2
Security Inprocessing and Outprocessing

2-1. HQ USAREC, HQ RS Bde, and RSB

a. Inprocessing. Directorate supervisors and SMs shall ensure all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided automation information systems (AISs) or access thereto inprocess with the HQ RS Bde Security Division upon assignment to the headquarters. The Security Division will verify security investigation and security clearance documentation and initiate actions to request appropriate security investigation or security clearance as required by duty position or career field. The Security Division shall provide and document initial security briefings for all incoming military personnel and newly appointed civilian personnel. Briefings will include security-related matters such as operations security, SAEDA, information security, and PHS. Security files for each individual will be established and maintained by the Security Division.

b. Outprocessing. Directorate supervisors and SMs shall ensure all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided AISs or access thereto outprocess through the Security Division prior to departure from the headquarters as a result of a permanent change of station, transfer, or termination of employment. The Security Division will verify that each individual has a record of appropriate security investigation or security clearance initiation or completion in their personnel file. The Security Division will notify the Headquarters Commandant, HQ USAREC, and the personnel service center if military personnel do not meet security clearance requirements for transfer. Security investigative or clearance documents required by the next duty assignment shall be prepared and forwarded as appropriate. Required security debriefing and termination statements will be completed and forwarded as required. Notification reports to personnel central clearance facility (CCF) will be prepared and forwarded as required.

2-2. Rctg Bde and Rctg Bn activities

a. Inprocessing. Commanders will ensure that all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided AISs or access thereto inprocess with the appointed SM within 24 hours of assignment to the activity.

(1) The SM will verify suitability and security investigation and security clearance documentation for each individual assigned and initiate actions to request appropriate suitability and security investigation or security clearance as required by duty position or career field.

(2) Initial security briefings shall be provided and documented for all incoming military personnel and newly appointed civilian personnel. Briefings will include security-related matters such as SAEDA, information security, and PHS. Security files for each individual will be established and maintained.

b. Outprocessing. Commanders will ensure all personnel, permanent, temporary, term, and volunteers, including military, civilians, and contractors using Government-provided AISs or access thereto outprocess with the appointed SM prior to departure from the activity as a result of a permanent change of station, transfer, or termination of employment. The SM shall verify each individual has a record of appropriate security investigation or security clearance initiation or completion. The SM will notify the activity commander and personnel service center if military personnel do not meet security clearance requirements for transfer. Security investigative or clearance documents required by the next duty assignment shall be prepared and forwarded as appropriate. Required security debriefings and termination statements will be completed and forwarded as required. Notification reports to CCF will be prepared and forwarded as required.

Chapter 3
PS

3-1. Suitability investigations and security

clearances
AR 380-67 as supplemented by written policy and guidance from the Department of Army Military Intelligence Counterintelligence and Security (DAMI-CIS) and CCF provide specific requirements for the PS Program. PS investigations; periodic reinvestigations; determination of clearance requirements; designation of civilian position sensitivity levels; initial, annual, and foreign travel security briefings; granting interim security clearances; granting access to classified information; reporting unfavorable information; denial and/or suspension of access to classified material; recommending revocation or denial of security clearance; and maintenance of security records and files are the responsibility of the HQ RS Bde Security Division for HQ USAREC, HQ RS Bde, and the United States Army Recruiting Support Battalion (RSB) personnel and that of Rctg Bde and Rctg Bn commanders and/or their appointed SMs for their respective activities. The HQ RS Bde Security Division and SMs at Rctg Bdes and Rctg Bns will only process and request security investigations, periodic reinvestigations, or security clearances for U.S. citizens in accordance with DA regulation and policy. Individuals will not be processed for a security investigation or security clearance without a valid requirement as described below:

a. Military (Army). Positions requiring specified investigative and/or clearance by military occupational specialty, branch or career management series, duty positions, specific automation data processing sensitivity, official assignment instructions, or official educational or travel requirements.

b. Civilians. Employee positions that have designated position sensitivities of noncritical sensitive or critical sensitive, those approved job descriptions requiring security clearances, official assignment instructions, or those specific instructions provided by Department of Defense (DOD) and DA agencies.

(1) Favorable completion of suitability investigation is a condition of employment for all civilian employees. This procedure is normally initiated by the servicing civilian personnel office and is basically used as a suitability determination. A final security clearance as required by the position or career specialty may be a condition of initial or continued employment by a Federal employee. Federal employees may be appointed pending completion of investigation and/or granting of final security clearances provided applicable procedures of AR 380-67 are followed.

(2) The RS Bde security officer and Rctg Bde and/or Rctg Bn SM are responsible for the approval and designation of civilian position sensitivity levels for their respective activities. Changes to existing sensitivity designations or approval of new sensitivity designations requires a copy of the job description, written justification for the need of a security clearance, and a completed SF 52-B (Request for Personnel Action) be routed through and approved by the RS Bde Security Division or the Rctg Bde or Rctg Bn security office prior to forwarding to the servicing civilian personnel office.

(3) In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with DOD 5200.2-R, appendix E, and AR 380-67, paragraphs 9-102b and 9-102c, as well as a comment regarding an employee's discharge of security responsibilities.

c. Contractors. Contractor employees, like all personnel accessing AISs, must have a completed suitability investigation prior to granting access to AISs. Investigations must be completed according to the designated automation data processing sensitivity level as described in AR 380-19, paragraph 2-16.

3-2. Security briefings
In addition to initial security briefings, the RS Bde security officer will prepare, conduct, and document overseas travel briefings, initial security briefings, and annual refresher briefings as required by AR 380-67, AR 381-12, and AR 380-5.

3-3. Officials authorized to grant security clearances
Only the Commander, CCF, may grant final security clearances. Final security clearances are documented on a CCF generated DA Form 873 (Certificate of Clearance and/or Security Determination). Commanders or their designated SMs (in writing) are the only individuals authorized to grant interim security clearances as authorized by the provisions of AR 380-67.

3-4. Suitability and entrance investigations
Required suitability and entrance investigations shall be conducted in accordance with the provisions of AR 380-67.

3-5. Requesting PS investigations
Requests for PS investigations shall be processed and forwarded by the commander or the appointed SM as outlined in AR 380-67, chapter 5.

3-6. Granting access to classified information
Access to classified information may be granted only by the HQ RS Bde Security Division for HQ USAREC, HQ RS Bde, and RSB. Rctg Bn commanders or their appointed SMs may grant access to personnel assigned to their activities provided that each individual meets the criteria established in AR 380-67, paragraph 7-102. Specific procedures for granting access to classified information are contained in AR 380-67, paragraph 7-102.

3-7. Reporting unfavorable information
AR 380-67, chapter 8, provides requirements for reporting unfavorable information. When a commander learns of credible derogatory information within the scope of AR 380-67, paragraph 2-200, the commander or appointed SM will complete and forward DA Form 5248-R (Report of Unfavorable Information for Security Determination) to the Commander, CCF. The HQ RS Bde Security Division will report credible derogatory information for all HQ USAREC activities, HQ RS Bde, and RSB.

3-8. Security education
Commanders will establish and implement security education and awareness programs in accordance with AR 380-67, chapter 9, section II.

3-9. PS records and data
Maintenance of individual PS records and rostered security information is an essential tool for the effective management of the PS Program. Information contained in security files or records, and on access or security rosters shall be protected according to the sensitivity of the information contained therein. As a minimum, commanders or their appointed security representative shall maintain:

a. Personal security records. A security file will be maintained for each individual assigned or attached to the activity. Contained in the file will be a verification by the commander or SM, as to the individual's investigative and/or clearance status as verified with the official investigative or clearance authority. In addition, records of clearance actions and correspondence, briefings, debriefings, reports of unfavorable information, local records checks, etc., will be maintained. Files will be maintained in accordance with AR 25-400-2 requirements. File contents are to be maintained until the individual is no longer assigned to the activity, at which time the contents will be destroyed by appropriate method.

b. Security data or rosters. Activity commanders or appointed SMs will maintain a current and up-to-date record or listing of all personnel assigned to their activity that reflects the current status of security investigation, clearance, and level of access granted. The listing may be generated from a computer database, typewritten, or handwritten. The listing must contain verification of security clearance and level of access granted and enough personal information, such as name, social security number, date of birth, place of birth, etc., to verify identification of an individual. The HQ RS Bde Security Division will maintain such information for all HQ USAREC activities, HQ RS Bde, and RSB.

Chapter 4
Information Security

4-1. General
Classified information and materials within USAREC will be handled, stored, transmitted, and destroyed in accordance with AR 380-5. Rctg Bde and Rctg Bn commanders are required to develop SOPs for this functional area as required by AR 380-5.

4-2. Document retention
The annual clean-out day, as required by AR 380-5, for all USAREC activities is the third Thursday of July. Each Rctg Bde commander will

notify, in writing, the HQ RS Bde Security Division of accomplishment of this requirement prior to 31 August of each calendar year.

4-3. SM appointments and responsibilities

a. The Commander, USAREC, will designate in writing an SM for USAREC as required by AR 380-5.

b. Requirement for designation of Rctg Bde, Rctg Bn, and directorate or activity SMs are established by paragraph 1-4c.

c. Specific SM responsibilities are provided in AR 380-5.

Chapter 5
SAEDA

5-1. General

SAEDA requirements for USAREC are established in AR 381-12.

5-2. SAEDA training

a. All USAREC personnel will receive an initial briefing during inprocessing and attend biennial SAEDA briefing. The commander or appointed SM will present initial briefing. Counterintelligence personnel, the commander, or appointed SM will present refresher SAEDA briefing(s) biennially (every 2 years) with the first briefing in fiscal year 1995. Subject matter requirements are determined in AR 381-12. SMs may receive assistance in preparing and presenting SAEDA instructions from the supporting military intelligence element and the HQ RS Bde Security Division.

b. Biennial SAEDA briefing requirements are not considered fulfilled unless antiterrorism training is included as part of the overall briefing.

c. Commanders or SMs will make every effort to prepare current, interesting, and relevant presentations. Individuals who are especially vulnerable to foreign intelligence agent approaches by virtue of their position, travel, duties, or activities will receive a special SAEDA briefing. Specific situations requiring a special SAEDA briefing are given in AR 381-12.

5-3. SAEDA reporting

Rctg Bde and Rctg Bn commanders or appointed SMs are required to provide the HQ RS Bde Security Division with information described in AR 381-12 no later than 25 days following the end of the fiscal year.

Chapter 6
PHS

6-1. General

AR 190-13 and AR 190-51 establish policies for protecting and safeguarding Government property. AR 190-13 identifies requirements for all tenant commanders. Additional requirements are established in this chapter.

6-2. Responsibilities

a. PHS is a commander's responsibility. The RS Bde security officer is responsible for PHS programs for HQ USAREC, HQ RS Bde, and RSB, and providing assistance, guidance, and support to Rctg Bde and Rctg Bn commanders. Rctg Bde and Rctg Bn commanders are responsible for PHS programs for their respective units.

b. PHS programs must provide the means to counter threat entities during peacetime, mobilization, and war. Commanders, supervisors, and individuals responsible for the use, transport, accountability, security, or possession of Government property shall take every precaution to ensure adequate security is provided for that property at all times. PHS measures employed must be adequate, reasonable, and economical. They must retard unauthorized access to information, material, and equipment and prevent interference with the operational capability of the activity. However, great care must be exercised to ensure security is not sacrificed for the sake of convenience. If doubt exists as to the standard being used to secure Government property, the HQ RS Bde Security Division will determine what the approved standard will be.

c. When deficiencies exist, commanders shall initiate reasonable compensatory measures until the deficiency is corrected. In those cases where a weakness may exist and property or equipment may be exposed, the use of constant surveillance (guards) is the best compensatory measure. Protection of the Government's interest and loss prevention are the goals of this policy. Inefficiency, procrastination, fraud, waste, and abuse lead to losses or create crime-conducive conditions.

6-3. PHS plans and reports

Commanders shall develop a PHS plan and PHS survey reports for their activities, as applicable, according to guidance provided in AR 190-13. A copy of these documents will be forwarded to the HQ RS Bde Security Division.

6-4. PHS equipment

Requests for PHS equipment such as intrusion detection systems, electronic entry control systems, and closed circuit television will be submitted to the HQ RS Bde Security Division for approval prior to issue, purchase, lease, or lease renewal.

6-5. USAREC facilities

Policies, procedures, and methods related to management of USAREC facilities are contained in USAREC Reg 405-1. Commanders must ensure that facilities continue to meet basic structure security requirements as established by AR 190-51. The safeguarding and protection of property and materials in the possession of USAREC activities will be provided as established by AR 190-13 and AR 190-51 or by compensatory measures as approved by the commander or the HQ RS Bde Security Division.

6-6. End-of-day security checks

When closing a USAREC-occupied building or separate office located in a building with more than one activity (section, division, department, agency, etc.,) at the end of the duty day, a designated person(s) will make a security check of the building or office to ensure all doors, windows, and other openings are properly secured and that containers storing controlled or pilferable items and sensitive or classified information are locked. Occupants of separate offices are responsible for conducting end-of-day security checks for their individual offices. Other items may be included as required by the commander or supervisor of the activity. Records of these security checks will be annotated on SF 701 (Activity Security Checklist). Where practical, SF 701 will be posted at the lockup door. When completed, SF 701 will be retained for 30 days.

6-7. Emergency notification cards

a. All tenant USAREC activities located on or in Government-owned or Government-leased properties shall follow the host activities procedures for use of emergency notification cards. Activities not located on Government-owned or Government-leased properties shall ensure notification information is posted on or adjacent to all entrances of buildings or on gates leading to the building. USAREC Form 810 (Emergency Notification Card) may be used. Activities located in areas where use of a language other than English is used as primary language shall include both English and the primary use language on the card. Cards are to be posted so as to protect against adverse weather conditions and vandalism (i.e., inside of doors or windows).

b. Where possible, every precaution should be taken to prevent the disclosure of individual names, addresses, and home telephone numbers of response personnel. Numbers of the unit, charge of quarters, staff duty officer, police, or security guard services should be used. Coordinating with and providing names, addresses, and home telephone numbers to the charge of quarters, staff duty officer, police, or other agencies may be necessary. When Privacy Act information must be included on the notification card, appropriate Privacy Act statement must also be included on the card.

6-8. PHS inspections

a. During annual facilities inspections conducted by the Rctg Bn commander, as directed by USAREC Reg 405-1, the commander shall also conduct an informal PHS inspection to ensure proper security measures are being employed to safeguard personnel, equipment, and material. Written results of the inspections, citing deficiencies, and recommended corrective measures will be maintained until the next inspection is conducted.

b. The USAREC security officer conducts announced and unannounced security inspections of HQ USAREC activities. The USAREC security officer may conduct announced security inspections at Rctg Bdes and Rctg Bns at intervals of at least once every 2 years. Results of inspections shall be prepared, forwarded, and maintained in accordance with AR 190-13.

c. Commanders will forward a copy of each PHS inspection conducted and any corrective actions taken or proposed by the commander on any USAREC facility within 30 days of the inspection to the HQ RS Bde Security

Division. This includes inspections conducted by the support installation or other inspecting activities (i.e., Federal Protective Service).

6-9. Security of funds and/or negotiable instruments

a. Commanders, supervisors, and individuals that handle, store, and transport funds are responsible for all such funds and shall take precautions to ensure the protection of funds. This will include, but is not limited to the following:

(1) Adequate storage sites and containers with limited access to fund storage areas, to include key or combinations to these sites and containers.

(2) Proper fund custodians are appointed with separation of functions and access.

(3) No mingling of official funds with coffee funds in the same container or cash box. Cash will not be stored in containers securing classified information.

b. The following minimum measures will be in effect for all activities that store cash or negotiable instruments on their premises on an overnight basis, unless otherwise provided for in other regulations.

(1) All funds that are secured on an overnight basis that are appropriated funds or are nonappropriated funds in excess of $200 will be secured in a tool resistant safe that is provided with a built-in three position dial combination lock that is equipped with a relocking device. Approved General Services Administration (GSA) security containers with Underwriter's Laboratory tool resistant ratings of TL-15 or higher may be used. If tool resistant money safes are not available, GSA approved Class 1 through 2, two-drawer security file containers may be used for the security of funds that are not in excess of $500. Approved GSA Class 3 through 6 security file containers, weighing in excess of 750 pounds, will be used for the security of funds that are over $500, but less than $3,000. Security file containers are authorized for fund storage only when there are no better containers available or when purchase of new tool resistant containers would not be cost effective.

(2) Funds that are less than $200, that are to be secured on an overnight basis, must be secured in an approved, lockable safe or steel container. Safes and containers that cost more than the amount of monies being secured within will not be purchased solely to conform to this regulation. Two-drawer Class 1, 2, and 6 security containers or Army field safes with built-in combination locks may be used for funds of less than $200.

(3) The use of small portable cash boxes for overnight storage is prohibited unless stored within approved containers as described in (1) and (2) above.

(4) Padlocks will not be used to secure fund safe doors after duty hours.

(5) All safes, weighing less than 750 pounds, will be secured to the structure by approved methods. One method is to secure the safe to the structure by use of steel eye-bolts anchored to the floor, with short lengths of chain (5/16 inch thickness) beneath the safe that are secured to the anchor with harden steel padlocks, or, by welding the safe to the anchor.

(6) Safes that are on wheels will have the wheels removed or will be bolted or secured to the structure in an approved manner.

(7) Fund containers will be secured in a locked room or building of a secure structure as described in AR 190-51 or, be in a room or structure that is under constant surveillance of duty personnel.

(8) Combinations to fund safes will be safeguarded, stored, and changed in accordance with AR 380-5.

6-10. Small computers and business machines

Desktop computers, calculators, typewriters, and similar machines are desirable objects and are highly susceptible to theft. Every effort will be made to ensure adequate security of such property. As a minimum, all such items will be accepted on a hand receipt by a responsible person within each office or activity and serial number inventories shall be conducted at least quarterly. Buildings or offices in which such items are stored or used will have adequate doors, windows, and locking devices. If located in rooms with lockable doors, the doors will be closed and locked at the close of business.

6-11. Mailrooms

Minimum security standards are located in DOD 4525.6-M, Volumes 1 and 2. Access control will be established and limited to unit mail personnel and the commander only. Signs will be posted on entrances to designate authorized entry only. SF 702 (Security Container Check Sheet) will be posted on the outside of all safes and containers containing certified or classified mail and on the outside of the entrance door. Certified and registered mail, as well as payroll checks, stamps, indicia, or other similar items will be as a minimum, secured in a field safe or similar container that is provided with a built-in combination lock or that can be secured by approved hasp and combination padlock. Safes or containers weighing less than 750 pounds must be secured to the structure by an approved method. Classified mail will be screened, accounted for, secured, and transported in accordance with AR 380-5.

6-12. Administrative key control

a. Control, accountability, and PHS of Government property are interdependent. A comprehensive key control and property accountability system are basic to an effective PHS Program. Control of locks and keys provides primary safeguards for Government property and assets.

b. The term administrative keys applies to all keys other than those for arm ammunitions and explosives, alarm systems, or special access keys which require a higher level of control. Implementation and supervision of administrative lock and key control shall be in accordance with AR 190-51. Rctg Bdes and Rctg Bns must develop written procedures for the control and accountability of all keys used to protect or secure Government property.

c. There are three approved USAREC forms to be used for the control and management of administrative keys by all USAREC activities. They are:

(1) USAREC Form 1191 (Master Key Inventory).

(2) USAREC Form 1192 (Key Sign-In and Sign-Out Record).

(3) USAREC Form 1193 (Key Inventory Log (Monthly and Semiannually)).

Chapter 7
Antiterrorism

7-1. General

a. Terrorism and counteraction. No person is immune from the threat of terrorism. Any representative of the U.S. Government is a possible object of terrorist activity. For this reason, every individual must develop a security-conscious attitude. AR 525-13 establishes requirements for terrorism directed against military personnel and property. Antiterrorist, hostage rescue, or hostage crisis plans are developed and implemented by the supporting AR 5-9 activity for USAREC activities (i.e., Fort Knox provides support for HQ USAREC in the Fort Knox Antiterrorist/Hostage Rescue Operations Plan). Rctg Bde and Rctg Bn commanders must ensure this functional area is included in their local ISA. Copies of such plans will be maintained at each command level.

b. Guidance in this chapter applies to all activities and personnel assigned or attached to USAREC. All employees are encouraged to provide information regarding terrorism to their family members.

c. Senior ranking personnel and recruiter personnel whose duties require operation outside of the normal Army or DOD communities will receive periodic briefings and/or training on the current threat and on precautions that can be taken to reduce their vulnerability to terrorist attacks. Antiterrorism training will be provided as established by AR 525-13.

d. All USAREC personnel must receive a Level II Antiterrorism briefing within 6 months of any outside the continental United States (OCONUS) travel, including permanent change of station and temporary duty. The Level II training must be conducted by the activities antiterrorism officer or an individual that has been certified to conduct Level II training. Rctg Bde and Rctg Bn personnel must receive a travel briefing conducted by the appointed Rctg Bde or Rctg Bn SM. This briefing describes known terrorist threats and protective measures for traveling OCONUS or to any area of high risk.

e. As a part of travel planning and protocol, coordination with the supporting federal or military law enforcement agencies must be conducted when individuals travel on official business to areas OCONUS or those areas considered high risk. This coordination must include considerations for protective measures and contingency plans that are in place by that location where the temporary duty or travel is to

be conducted.

7-2. Responsibilities

a. The Department of State has the primary responsibility for dealing with terrorism involving Americans abroad and for handling foreign relations aspects of domestic terrorism incidents.

b. The Department of Justice is the primary agency for coping with domestic terrorism. Investigative and operational responsibility rests with the Federal Bureau of Investigation (FBI) who has overall responsibility for combating and investigating domestic terrorism including the District of Columbia, the Commonwealth of Puerto Rico, and US possessions and territories.

c. In the US the installation commander has responsibility for the maintenance of contingency plans for use of security forces to isolate, contain, and neutralize a terrorist incident within the capability of the installation resources. The installation commander provides initial and immediate response to any incident occurring on a military installation. The FBI is immediately notified and, if jurisdiction is assumed, the Attorney General assumes responsibility for coordinating the Federal law enforcement response. If the FBI does not assume jurisdiction, the military commander will take actions to resolve the incident.

d. Rctg Bde and Rctg Bn commanders must incorporate applicable provisions of AR 525-13, supporting installation policy, and this chapter into SOPs for their activities. Commanders must ensure that all personnel, including family members, are aware of the potential threat of terrorism and take all measures practical to provide adequate physical protective measures, training, and information regarding terrorist and criminal threats.

e. The USAREC or supporting installation public affairs officer (PAO) must be included in all reporting actions related to terrorist incidents. The PAO is the sole spokesperson and release authority for information regarding a terrorist incident for the commander until such time as the responsibility for counterterrorism operations is transferred to another Federal agency. The Rctg Bn PAO will immediately notify the Rctg Bde PAO and the HQ USAREC, Director of Advertising and Public Affairs, if an act of terrorism occurs at a USAREC facility. The Director of Advertising and Public Affairs will then notify the HQ RS Bde Security Division and appropriate Headquarters, Department of the Army (HQDA) activities as required by AR 525-13.

7-3. Terrorism

No specific terrorist organization is known to be targeted against USAREC facilities. However, acts of terrorism against USAREC activities have been conducted by antigovernment or antimilitary groups. The unprotected or "open" status of the numerous USAREC facilities and recruiting stations require members of USAREC to become keenly aware of their surroundings and indicators of terrorist or subversive activities on a continuous basis. Commanders at all levels must coordinate with their supporting activity for information regarding current threats and review organizational security plans, regulations, policies, applicable PHS countermeasures, and procedures to be employed to deter and counteract a terrorist incident.

7-4. Terrorist Threat Conditions

a. Information and warnings of terrorist activity against installations and personnel of US commands and agencies will normally be received from US security authorities or through the security agencies of host countries concerned. Information may come from local police forces, be received directly by a US command or agency as a threat or warning from a terrorist organization, or be in the form of an actual attack on US personnel or property.

b. Terrorist Threat Conditions (THREATCON) declaration and implementation measures. The declaration of a THREATCON, as identified by AR 525-13 and implementation of applicable measures may be decreed by any USAREC commander above Rctg Co level for any activity of his or her command that does not share facilities with other Federal or foreign organizations. If activities share facilities or are tenants of other installations, declaration and implementation must be coordinated with these supporting organizations.

7-5. Reporting requirements

a. Should individuals become involved in or have knowledge of a terrorist incident, immediately report the incident to the local military police if located on a military installation, local civilian police or FBI if not located on a military installation.

b. Rctg Bde and/or Rctg Bn commanders declaring or in receipt of a declaration of THREATCON higher than NORMAL (no threat) (i.e., ALPHA (low threat), BRAVO (medium threat), CHARLIE (high threat), and DELTA (imminent threat)), will immediately report changes to the HQ USAREC Emergency Operations Center (EOC), both telephonically at (502) 626-0823 or 0825 (facsimile) or DSN 536-0823 or 0825 (facsimile) and as an incident report as required in chapter 9. In addition, reports required by the supporting installation must be provided. Actual terrorist incidents involving USAREC personnel will be reported in the same manner.

c. HQ USAREC will respond as required to THREATCON declarations as issued by the Commander of Fort Knox for HQ USAREC. The HQ USAREC EOC will report changes to commander decreed THREATCON levels to the HQ USAREC PAO (coordination) and to appropriate HQDA activities as required by AR 525-13. The HQ USAREC antiterrorism officer will coordinate actions to ensure any actual terrorist incident involving USAREC personnel has been or is reported to the appropriate higher authority.

Chapter 8
Bomb Threats

8-1. Bomb threat procedures

a. A bomb incident control officer (BICO) will be designated, in writing, for every command level down to Rctg Bn. The HQ USAREC EOC is the command point of contact for bomb threat procedures. The Headquarters Commandant, HQ USAREC, is designated the BICO and PHS officer for all headquarters buildings, assets, and personnel. A copy of appointments for PHS officer and BICO will be forwarded to the HQ USAREC EOC. Minimum grade requirements for these positions will be a commissioned officer or civilian in the grade of GS-09 or above. Guidance for bomb threats is contained in FM 3-19.30.

b. All bomb threats will be treated as actual until it has been determined to be otherwise and the "ALL CLEAR" has been given by the explosive ordnance disposal or law enforcement personnel with overall authority for bomb search. A bomb threat is a message delivered by any means, warning or claiming the presence of one or more bombs or explosive devices. A bomb threat may or may not specify the location of a bomb; it may or may not contain an ultimatum related to the detonation, ignition, or concealment of the bomb.

c. Commanders shall develop procedures that address the particular circumstances and operational needs of the unit or activity should a bomb threat occur. These procedures should identify supporting activity requirements, coordination, and procedures. The procedures include:

(1) Appointment and responsibilities of BICOs.

(2) Notification procedures to be followed upon receipt of the bomb threat.

(3) Procedures for evacuation.

(4) Criteria for evacuation of sensitive areas.

(5) Security during and after the evacuation.

(6) Predesignated assembly areas.

(7) Search procedures and designation of search team members.

(8) Establishment of emergency coordination point.

(9) Training of personnel, to include classes by explosive ordnance disposal personnel on the recognition of various bombs and devices.

(10) Afteraction reporting procedures.

(11) Ensuring buildings are inspected on a regular basis so search teams become familiar with places within and outside of the buildings where a bomb may be placed.

(12) Posting of FBI Form 2-182A (Bomb Threat) under each telephone instrument in the activity.

8-2. Reporting procedures

a. HQ USAREC, HQ RS Bde, and RSB. All individuals assigned or attached to HQ USAREC, HQ RS Bde, and RSB must report any suspicious events, matters, and unauthorized personnel to their immediate supervisor and the HQ USAREC EOC.

b. Rctg Bdes and Rctg Bns. Commanders will report acts of terrorism and bomb threats to the HQ USAREC EOC as outlined in chapter 7. Supplemental information regarding terrorism against recruiting activities will be reported on the hour every 2 hours for the duration of the incident. In addition, the recruiting advertising

and public affairs chief will be immediately notified if an act of terrorism occurs. The PAO is the sole spokesperson for the commander until such time as the responsibility is transferred to another Federal agency. Requests for information or statements from the news media outside the immediate area of the USAREC facility subject to a terrorist incident will be handled by the HQ USAREC PAO.

Chapter 9
Serious Incidents

9-1. Serious incident reports

a. A serious incident is an actual or alleged incident, accident, misconduct, act, or condition (either criminal or noncriminal) that warrants timely notice to HQDA because of its nature, gravity, publicity, or potential consequences.

b. Serious incidents reports (SIRs) are law enforcement reports submitted by an installation commander (provost marshal) having geographic responsibility as established in AR 5-9. SIRs are forwarded to HQDA (DAMO-ODL) by provost marshals. No USAREC activities are authorized to send SIRs to HQDA. However, USAREC activities shall provide information to the installation commander having geographic responsibility for all reportable incidents as described in AR 190-40 and this regulation.

c. The HQ USAREC EOC shall receive, process, and distribute reported incidents according to internal staff instructions and requirements. The EOC shall be the primary activity responsible for forwarding incident reports to higher headquarters as necessary. During duty hours the EOC shall make required distribution immediately upon receipt of the incident. During nonduty hours notification procedures and distribution shall be made according to special duty instructions. The EOC shall be the primary activity responsible for ensuring information reported adequately describes events, circumstances, and details regarding the incident being reported, obtaining clarification or additional information from the reporting activity as necessary. The EOC is the primary activity to solicit information from the reporting activity for clarification, additional details, and/or followup information for any previously reported incident. Notification procedures for key personnel regarding subject matter or specific categories of incidents that are of immediate concern shall be provided as special instructions. Immediately after receipt of an incident report the EOC shall provide a copy of each reported incident to each activity listed on the current approved distribution matrix.

9-2. Categories of incidents

AR 190-40, appendixes B and C, establishes two categories (Category 1 and 2) of incidents that will be reported to HQDA (DAMO-ODL). Category 1 and 2 incidents will also be reported to HQ USAREC. Category 3 incidents shall be reported only to USAREC.

a. Category 1. Category 1 incidents as described by AR 190-40, appendix B, shall be reported immediately upon discovery or notification to both HQDA and HQ USAREC. Notification of incidents will not be delayed due to incomplete information. Commanders shall review AR 190-40, appendix C, for all items that are reportable. Category 1 incidents that may occur within USAREC are as follows:

(1) On- and off-post riots, serious disturbances, or demonstrations targeted against the Army or involving Army personnel.

(2) Terrorists activities, sabotage, and incidents initiated or sponsored by known terrorists, dissident groups, or criminal elements that occur on an installation or involve military personnel or property off an installation.

(3) Bomb or explosive incidents resulting in death, injury of military personnel, or damage to military property.

(4) Incidents involving material damage that seriously degrade unit operations or training readiness.

(5) Any other incident that the commander determines to be of immediate concern to HQDA based on nature, gravity, potential for adverse publicity, or potential consequences of the incident.

b. Category 2. Category 2 incidents are described by AR 190-40, appendix C. Incidents shall be reported to the installation commander (provost marshal) having geographic responsibility within 24 hours of discovery or notification and immediately to HQ USAREC. Notification of incidents will not be delayed due to incomplete information. Commanders shall review AR 190-40, appendix C, for all items that are reportable. Category 2 incidents that may occur within USAREC are as follows:

(1) Significant violations of Army standards of conduct, to include bribery, conflict of interest, graft, or acceptance of gratuities by soldiers or DA or nonappropriated fund employees.

(2) Aggravated arson.

(3) Deaths, to include homicides, suicides, and death resulting from traffic accidents, training accidents, fires, or other incidents.

(4) Kidnapping.

(5) Major fires or natural disasters involving death, serious injury, property damage in excess of $100,000, or damage that seriously degrades unit operational or training capabilities.

(6) Incidents involving firearms that cause injury or death.

(7) Any other incident that the commander determines to be of immediate concern to HQDA based on nature, gravity, potential for adverse publicity, or potential consequences.

c. Category 3. Other incidents that may cause unfavorable publicity or otherwise be of concern to HQ USAREC that involve USAREC personnel (both military and civilian) family members, facilities, or property which shall be reported to HQ USAREC.

(1) The following incidents will be reported to HQ USAREC immediately upon discovery or notification:

(a) Death of USAREC personnel or family members (spouse, children, and/or permanent members of household).

(b) Attempted suicide.

(c) Bomb threats or explosions.

(d) Terrorist threats and assaults to recruiters, family members, or facilities.

(e) Demonstrations.

(f) Felony arrests involving recruiting personnel.

(g) Reduced operational capability due to natural disaster or loss of facilities or equipment.

(h) Actual or potential adverse publicity regardless of media source.

(i) All matters or incidents referred to the United States Army Criminal Investigation Command (CID) for investigation or review.

(2) The following incidents will be reported to HQ USAREC within 24 hours of discovery or notification:

(a) Any incident of child abuse, spouse abuse, and/or domestic altercations.

(b) Drug or alcohol abuse to include positive urinalysis results and/or driving under the influence or driving while intoxicated.

(c) Hospitalization of service member or family member (spouse, children, and/or permanent member of household) due to life threatening injury or illness.

(d) Sexual misconduct.

(e) Damage, theft, or vandalism of Government facilities and equipment.

(f) Misdemeanor arrests involving recruiting personnel.

(g) Alleged or confirmed incidents, whether recently committed, or just surfacing that occurred several months or years earlier that were not previously reported, must be reported to this headquarters.

(h) Sexual harassment.

(i) Any other incident that the commander determines to be of immediate concern to HQ USAREC based on nature, gravity, potential for adverse publicity, or potential consequences of the incident.

9-3. Category 1 reporting procedures

a. Reporting information for HQDA. The USAREC Rctg Bn commander or the USAREC Rctg Bde commander if involving personnel assigned to the Rctg Bde headquarters shall immediately notify, via telephone, the responsible installation provost marshal. The telephonic report shall be in accordance with instructions of AR 190-40, figure 3-1, and in the format in AR 190-40, figure 3-4. Followup information and final disposition of the incident shall be provided as additional information becomes available or as requested by the reporting provost marshal. The responsible installation provost marshal makes a formal law enforcement report to HQDA.

b. Reporting information to HQ USAREC. In addition to reporting requirements of a above, the Rctg Bn commander shall immediately report Category 1 incidents involving personnel assigned to HQ USAREC as described below. The Rctg Bde commander shall immediately report Category 1 incidents involving personnel assigned to the Rctg Bde headquarters as described below.

(1) The commander (Rctg Bn or Rctg Bde) shall immediately notify the Commanding General (CG) (24 hours a day, 7 days a week), by telephone, of all incidents involving the death of

USAREC personnel or family members (spouse, children, or other permanent members of the household) or other incidents that have had or may have a serious negative impact on the command. In addition, follow the procedures described in (2) through (6) below.

(2) Immediately send, via e-mail, a spot report to HQ USAREC Command Group (CG, Deputy Commanding General (DCG)-East, DCG-West, Chief of Staff (CofS), Secretary of the General Staff (SGS), Command Sergeant Major, and the HQ USAREC EOC) for incidents involving death or life threatening injury of USAREC personnel or immediate family members, attempted suicide, terrorist threats, or assaults on USAREC personnel or family members (spouse, children, or other permanent members of the household), demonstrations, felony arrest, actual or potential adverse publicity, bomb threats or explosions, and all matters or incidents referred to CID. In addition, follow procedures described in (1) above and (3) through (6) below.

(3) During HQ USAREC's normal duty hours, immediately notify the SGS, by telephone, of all incidents requiring immediate reporting to either HQDA or HQ USAREC. During HQ USAREC's nonduty hours immediately notify the HQ USAREC EOC, by telephone, of all incidents requiring immediate reporting to either HQDA or HQ USAREC.

(4) Telephonically notify the HQ USAREC EOC of the incident prior to transmitting the report. A completed USAREC Form 958 (Incident Information Report) shall be forwarded via facsimile to the EOC. All incident reports shall be forwarded to the HQ USAREC EOC at (502) 626-0823 or DSN 536-0823; fax (502) 626-0825 or DSN 536-0825. Rctg Bn and Rctg Bde commanders must ensure that telephonic notification is provided to the EOC immediately upon obtaining knowledge of all other incidents requiring immediate reporting, and those incidents that have had or may have a serious negative impact on the command.

(5) Followup reports shall be submitted when additional information is known, when situation changes, when requested by the EOC or staff representative, or every 30 days until the action is completed and a final report has been submitted. The initial report and all subsequent followup reports must be provided with each new or additional followup and/or final report. Use of the initial report as a continuation page with additional pages is acceptable and recommended.

(6) A final report is required for all incidents.

9-4. Category 2 reporting procedures

A complete list of Category 2 incidents are described in AR 190-40. To ensure both HQDA and HQ USAREC are notified, the following reporting procedures shall be followed:

a. Reporting information for HQDA. Incidents shall be reported to the responsible installation commander (provost marshal) within 24 hours of discovery or notification. Incidents shall be made telephonically unless otherwise notified by the supporting provost marshal. Instructions and format are contained in AR 190-40. Followup information and final disposition of the incident shall be provided as information becomes available, final disposition, or as requested by the reporting provost marshal. The responsible installation provost marshal makes a formal law enforcement report to HQDA.

b. Reporting information to HQ USAREC. In addition to reporting requirements of a above, the Rctg Bn commander shall immediately report Category 2 incidents involving personnel assigned to HQ USAREC as described below. The Rctg Bde commander shall immediately report Category 2 incidents involving personnel assigned to the Rctg Bde headquarters as described below.

(1) The commander (Rctg Bn or Rctg Bde) shall immediately notify the CG (24 hours a day, 7 days a week), by telephone, of all incidents involving the death of USAREC personnel or family members (spouse, children, or other permanent members of the household) or other incidents that have had or may have a serious negative impact on the command. In addition, follow the procedures described in (2) through (6) below.

(2) Immediately send, via e-mail, a spot report to HQ USAREC Command Group (CG, DCG-East, DCG-West, CofS, SGS, Command Sergeant Major, and the HQ USAREC EOC) for incidents involving death or life threatening injury of USAREC personnel or immediate family members, attempted suicide, terrorist threats, or assaults on USAREC personnel or family members (spouse, children, or other permanent members of the household), demonstrations, felony arrest, actual or potential adverse publicity, bomb threats or explosions, and all matters or incidents referred to CID. In addition, follow the procedures described in (1) above and (3) through (6) below.

(3) During HQ USAREC's normal duty hours, immediately notify the SGS, by telephone, of all incidents requiring immediate reporting or reporting within 24 hours to HQDA and/or those incidents requiring immediate reporting to HQ USAREC. During HQ USAREC's nonduty hours immediately notify the HQ USAREC EOC, by telephone, of all incidents requiring immediate reporting to either HQDA or HQ USAREC.

(4) Telephonically notify the HQ USAREC EOC of the incident prior to transmitting the report. A completed USAREC Form 958 shall be forwarded via facsimile to the EOC. All incident reports shall be forwarded to the HQ USAREC EOC at (502) 626-0823 or DSN 536-0823; fax (502) 626-0825 or DSN 536-0825. Rctg Bn and Rctg Bde commanders must ensure that telephonic notification is provided to the EOC immediately upon obtaining knowledge of all other incidents requiring immediate reporting, and those incidents that have had or may have a serious negative impact on the command.

(5) Followup reports shall be submitted when additional information is known, when situation changes, when requested by the EOC or staff representative, or every 30 days until the action is completed and a final report has been submitted. The initial report and all subsequent followup reports must be provided with each new or additional followup and/or final report. Use of the initial report as a continuation page with additional pages is acceptable and recommended.

(6) A final report is required for all incidents.

9-5. Category 3 reporting procedures

a. Reporting information for HQDA. None required.

b. Reporting information to HQ USAREC. There are two reporting time lines established for Category 3 incidents. Paragraph 9-2c prescribes what incidents shall be reported immediately and within 24 hours to HQ USAREC. Included in Category 3 are incidents that require immediate (deaths of military and civilian personnel) and within 24 hours (demonstrations and bomb explosions) reporting to HQDA. The Rctg Bn commander shall report Category 3 incidents as described by paragraph 9-2c involving personnel assigned to HQ USAREC as described below. The Rctg Bde commander shall immediately report Category 3 incidents as described by paragraph 9-2c involving personnel assigned to the Rctg Bde headquarters as described below.

(1) Telephonically notify the HQ USAREC EOC of the incident prior to transmitting the report. A completed USAREC Form 958 shall be forwarded via facsimile to the EOC. All incident reports shall be forwarded to the HQ USAREC EOC at (502) 626-0823 or DSN 536-0823; fax (502) 626-0825 or DSN 536-0825. Rctg Bn and Rctg Bde commanders must ensure that telephonic and USAREC Form 958 notification is provided to the EOC immediately or within 24 hours of obtaining knowledge of all other incidents as described in paragraph 9-2c(2).

(2) Followup reports shall be submitted when additional information is known, when situation changes, when requested by the EOC or staff representative, or every 30 days until action is completed and a final report has been submitted. The initial report and all subsequent followup reports must be provided with each followup and/or final report. Use of the initial report as a continuation page with additional pages is acceptable.

(3) Final reports are required for all reported incidents.

9-6. Additional requirements

In addition to the above, the following procedures are noted for reemphasize:

a. Commanders shall designate a primary and an alternate to report serious incidents to appropriate activities as outlined in this chapter.

b. Alleged or confirmed incidents, whether recently committed or just surfacing that occurred several months or years earlier must be reported to this headquarters.

c. Reports concerning Delayed Entry Program and Delayed Training Program personnel involving serious injury or death as well as any that may involve recruiting improprieties should be made to this headquarters.

d. Credible derogatory information must also be forwarded by the commander or SM through security channels on DA Form 5248-R to the U.S. Army Central Personnel Security Facility, ATTN: PCCF-M, Fort George G. Meade, MD 20755-5250. Reporting requirements are established by AR 380-67.

e. All matters coming to your attention as a possible crime must be reported to the local CID office.

Appendix A
References

Section I
Required Publications

AR 5-9
Area Support Responsibilities. (Cited in paras 7-1a and 9-1b.)

AR 25-400-2
The Modern Army Recordkeeping System (MARKS). (Cited in para 3-9a.)

AR 190-13
The Army Physical Security Program. (Cited in paras 6-1, 6-3, 6-5, and 6-8b.)

AR 190-40
Serious Incident Report. (Cited in paras 9-1b, 9-2, 9-2a, 9-2b, 9-3a, 9-4, and 9-4a.)

AR 190-51
Security of Unclassified Army Property (Sensitive and Nonsensitive). (Cited in paras 6-1, 6-5, 6-9b(7), and 6-12b.)

AR 380-5
Department of the Army Information Security Program. (Cited in paras 3-2, 4-1, 4-2, 4-3a, 4-3c, 6-9b(8), and 6-11.)

AR 380-19
Information Systems Security. (Cited in para 3-1c.)

AR 380-67
The Department of the Army Personnel Security Program. (Cited in paras 3-1, 3-1b(1), 3-1b(3), 3-2, 3-3, 3-4, 3-5, 3-6, 3-7, 3-8, and 9-6d.)

AR 381-12
Subversion and Espionage Directed Against the U.S. Army (SAEDA). (Cited in paras 3-2, 5-1, 5-2a, 5-2c, and 5-3.)

AR 525-13
Antiterrorism. (Cited in paras 7-1a, 7-1c, 7-2d, 7-2e, 7-4b, and 7-5c.)

DOD 4525.6-M, Volume 1
DOD Postal Manual. (Cited in para 6-11.)

DOD 4526.6-M, Volume 2
DOD Postal Manual. (Cited in para 6-11.)

DOD 5200.2-R
Department of Defense Personnel Security Program. (Cited in para 3-1b(3).)

FM 3-19.30
Physical Security. (Cited in para 8-1a.)

USAREC Reg 405-1
Facility Management. (Cited in paras 6-5 and 6-8.)

Section II
Related Publications

AR 15-6
Procedures for Investigating Officers and Boards of Officers.

AR 25-55
The Department of the Army Freedom of Information Act Program.

AR 40-2
Army Medical Treatment Facilities General Administration.

AR 50-5
Nuclear and Chemical Weapons and Materiel-Nuclear Surety.

AR 50-6
Nuclear and Chemical Weapons and Material, Chemical Surety.

AR 190-5
Motor Vehicle Traffic Supervision.

AR 190-11
Physical Security of Arms, Ammunition and Explosives.

AR 190-22
Searches, Seizures and Disposition of Property.

AR 380-10
Foreign Disclosure, Technology Transfer, and Contacts With Foreign Representatives.

AR 380-19-1
(O) Control of Compromising Emanations (U).

AR 530-1
Operations Security (OPSEC).

AR 600-37
Unfavorable Information.

AR 604-10
Military Personnel Security Program.

AR 614-200
Enlisted Assignments and Utilization Management.

AR 635-200
Enlisted Personnel.

AR 680-29
Military Personnel - Organization and Type of Transaction Codes.

AR 735-5
Policies and Procedures for Property Accountability.

DA Pam 190-12
Military Working Dog Program.

DA Pam 190-51
Risk Analysis for Army Property.

DA Pam 710-2-1
Using Unit Supply System (Manual Procedures).

DA Pam 710-2-2
Supply Support Activity Supply System: Manual Procedures.

(O) DOD 2000.12-H
Protection of DOD Personnel and Activities Against Acts of Terrorism and Political Turbulence.

DOD 5200.1-PH-1
Classified Information Nondisclosure Agreement (SF 312), Briefing Pamphlet.

DOD 5220.22-R
Industrial Security Regulation.

DOD 5400.7-R
DOD Freedom of Information Act Program.

FM 19-10
The Military Police Law and Order Operations.

FM 19-15
Civil Disturbances.

TB 5-6350-264
Selection and Application of Joint-Services Interior Intrusion Detection System (J-SIIDS).

Section III
Prescribed Forms

USAREC Form 810
Emergency Notification Card. (Cited in para 6-7a.)

USAREC Form 958
Incident Information Report. (Cited in paras 9-3b(4), 9-4b(4), and 9-5b(1).)

USAREC Form 1191
Master Key Inventory. (Cited in para 6-12c(1).)

USAREC Form 1192
Key Sign-In and Sign-Out Record. (Cited in para 6-12c(2).)

USAREC Form 1193
Key Inventory Log (Monthly and Semiannually). (Cited in para 6-12c(3).)

Section IV
Referenced Forms

DA Form 873
Certificate of Clearance and/or Security Determination.

DA Form 5248-R
Report of Unfavorable Information for Security Determination.

FBI Form 2-182A
Bomb Threat.

SF 52-B
Request for Personnel Action.

SF 701
Activity Security Checklist.

SF 702
Security Container Check Sheet.

Glossary

AIS
automation information system

BICO
bomb incident control officer

CCF
central clearance facility

CG
Commanding General

CID
United States Army Criminal Investigation Command

CofS
Chief of Staff

DA
Department of the Army

DCG
Deputy Commanding General

DOD
Department of Defense

EOC
Emergency Operations Center

FBI
Federal Bureau of Investigation

GSA
General Services Administration

HQDA
Headquarters, Department of the Army

HQ RS Bde
Headquarters, United States Army Recruiting Support Brigade

HQ USAREC
Headquarters, United States Army Recruiting Command

ISA
installation support agreement

OCONUS
outside the continental United States

PAO
public affairs officer

PHS
physical security

PS
personnel security

Rctg Bde
recruiting brigade

Rctg Bn
recruiting battalion

Rctg Co
recruiting company

RS Bde
United States Army Recruiting Support Brigade

RSB
United States Army Recruiting Support Battalion

SAEDA
Subversion and Espionage Directed Against the U.S. Army

SGS
Secretary of the General Staff

SIR
serious incident report

SM
security manager

SOP
standing operating procedure

THREATCON
Terrorist Threat Conditions

USAREC
United States Army Recruiting Command